RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 6 / 20. November 2012

AUFGABE 1:
Sei $M \in \mathbb{N}$ mit unbekanntem Teiler b und $f(x) \in \mathbb{Z}_M[x]$ mit Grad n. Sei $\mathcal{A}$ ein Algorithmus, der bei Eingabe M und $f(x)$ eine Nullstelle x_0 von $f(x)$ modulo b berechnet, die keine Nullstelle von $f(x)$ modulo M ist, d.h.

$$f(x_0) = 0 \bmod b \quad \text{und} \quad f(x_0) \neq 0 \bmod M.$$

Dann kann man einen nicht-trivialen Faktor von M in Zeit polynomiell in n und $\log M$ bestimmen.

AUFGABE 2:
Sei $N = pq$ ein RSA-Modul mit $p > q$. Sei $k \in \mathbb{N}$ eine unbekannte Zahl, die kein Vielfaches von q ist. Weiterhin sei eine Approximation $\widetilde{kp}$ von kp gegeben mit

$$|kp - \widetilde{kp}| \leq N^{\frac{1}{4}}.$$

Zeigen Sie, dass die Faktorisierung von N in Zeit polynomiell in $\log N$ berechnet werden kann.

Hinweis: Orientieren Sie sich am Beweis von Satz 69.

AUFGABE 3:
Sei (p, q, α, β) der öffentliche und a der geheime Schlüssel für das DSA-Signaturverfahren. Es sei $\text{sig}_k(x)$ die Signierfunktion, d.h.

$$\text{sig}_k(x) = (\gamma, \delta) = ((\alpha^r \bmod p) \bmod q, r^{-1}(x + a\gamma) \bmod q)$$

für eine Nachricht $x \in \mathbb{Z}_q^*$ und zufälliges $r \in_R \mathbb{Z}_q^*$. Zeigen Sie:

(a) Ist r bekannt, so kann man a effizient berechnen (sofern $\gamma \neq 0$).

(b) Sind $\text{sig}_k(x)$ und $\text{sig}_k(x')$ für $x \neq x' \bmod q$ mit gleichem r gegeben, so kann man a effizient berechnen (sofern $\gamma \neq 0$).

Hinweis: Für Teil (b) reicht es, r zu berechnen und Teil (a) anzuwenden.